

## **MEMORANDUM OF UNDERSTANDING ON NATIONAL SECURITY CASES (DPA)**

- (A) This Memorandum of Understanding (“the National Security MoU (DPA)”) between the Secretary of State for Justice (on behalf of Government Departments) and the Information Commissioner, sets out guidelines on the handling of national security cases (as defined in Recital (B) below) in the context of the Data Protection Act 1998 (“the DPA”).
- (B) Specifically, these guidelines provide for co-operation between Government Departments and the Information Commissioner in the operation of sections 42 and 43 of the DPA, insofar as they relate to cases where the exemption in section 28 has been relied on in response to a subject access request (“national security cases”).
- (C) This Memorandum of Understanding describes the respective roles of the Information Commissioner and Government Departments under the DPA in relation to national security cases.
- (D) This Memorandum of Understanding replaces, with reference to the DPA, the previous Memorandum of Understanding that was signed by Lord Falconer, the then Secretary of State for the Department of Constitutional Affairs, and Richard Thomas, the Information Commissioner, on 24 February 2005.

## **Purpose of the National Security MoU (DPA)**

1. The purpose of this MoU is to promote good standards of co-operation between Departments and the Commissioner in national security cases, that is to say in cases where:
  - (a) the exemption in section 28 of the DPA has been relied on to refuse the disclosure of personal data under a subject access request. It is recognised that s.28 covers situations other than Subject Access Requests, to which this MoU does not apply; or
  - (b) the exemption in section 28 of the DPA has been relied on to support a “Neither Confirm Nor deny” response; and
  - (c) a request has been made to the Commissioner for an assessment under section 42 of the DPA, or the Commissioner is considering serving a notice under sections 40 or 43 of the DPA.
2. This MoU does not apply in situations in which only one or more of the other exemptions in the DPA are being relied on.
3. The Definitions in the Annex apply to this MoU. This MoU sets out guideline procedures designed to apply to national security cases generally.
4. This MoU takes effect subject to the DPA and any other relevant legal provisions, and should be read alongside the relevant Codes of Practice. For the avoidance of doubt, nothing in this MoU will operate to restrict or otherwise inhibit the exercise of the powers and duties of the Commissioner or of Departments under the DPA.
5. This MoU seeks to minimise the costs of complying with the DPA, and to promote the efficient administration of the respective requirements of this legislation within Departments and the Commissioner's Office. However this is secondary to the proper fulfilment of the Commissioner's functions under the DPA.

6. It is recognised that, in order to discharge his important regulatory functions, where:

- (a) a person directly affected by processing of their personal data makes a request for an assessment under section 42 of the DPA (following a refusal by a Department to provide information in response to a subject access request under section 7 of the DPA); or
- (b) a Neither Confirm Nor Deny response is given to the requester,

the Commissioner has to satisfy himself that the relevant exemptions justifying non-disclosure and/or the Neither Confirm Nor Deny response have been properly relied on.

7. It is also recognised that national security cases will normally be particularly sensitive and it is accepted that the sensitivity of such cases means that there will often be a need for greater dialogue between the Commissioner and Departments before the Commissioner reaches any final conclusions.

#### **Steps to be taken where an application is made for an Assessment under section 42 of the DPA**

8. The Commissioner will contact the relevant Department(s) (via the nominated contact, where known) when he receives an application under section 42 of the DPA relating to a national security case, as soon as practicable and where possible within 20 working days of such receipt. At this time he will:

- (a) provide the Department with details of the Complainant's application;
- (b) request the Department to provide a reasoned explanation which justifies the application of the relevant exemption in the particular case as at the time of the request, together with any relevant background information;
- (c) invite the nominated contact to comment on the case;
- (d) aim to establish a single channel of communication.

If national security exemptions are claimed at a later stage, the Department should inform the ICO in writing as soon as possible.

9. The Department will:

- (a) provide the reasoned explanation, together with any additional relevant background information, as quickly as possible and, in any event, within 20 working days of being contacted by the Commissioner, unless the Commissioner otherwise agrees;
- (b) provide any additional relevant background information subsequently requested by the Commissioner as quickly as possible and in any event, unless the Commissioner otherwise agrees, within 20 working days of it being requested; and
- (c) inform the Commissioner, giving reasons, where it is not able to provide the reasoned explanation and other relevant information within the time periods set out in this paragraph and provide an indication of when it expects to be able to do so.

10. The reasoned explanation referred to in paragraphs 8 and 9 above:

- (a) in cases where the exemption in section 28 of the DPA is relied on by the Security and Intelligence Agencies, will confirm whether or not personal data is held. If data is so held the Agency will explain that the personal data falls within one of two categories of information, namely categories A or B. Categories A and B are defined as follows:
  - A. Information relating to covert operations or investigations by the Security and Intelligence Agencies which, if released, would jeopardise the aforementioned operation or investigations, or the ability of the Security and Intelligence Agencies to mount a similar operation or investigation in the future;

Information relating to methods or techniques employed by the Security and Intelligence Agencies which, if released, would jeopardise the current or future effectiveness of those methods or techniques;

Information relating to sources of information or intelligence (such as liaison services, human agents or technical sources) which, if disclosed, would jeopardise the provision of information or intelligence from these sources in the future.

B. Information relating to the structure and/or administration of the Security and Intelligence Agencies which, if disclosed, would jeopardise the effective execution of the statutory functions of the these Agencies;

Information relating to the identity, appearance, deployment or training of current and former members of the Security and Intelligence Agencies, the disclosure of which would endanger or risk endangering them or other individuals or would impair or risk impairing their ability to operate effectively as members of these Agencies or the ability of these Agencies to recruit and retain staff in the future;

- (b) in cases where the exemption in section 28 of the DPA is relied on by a government department (other than the Security and Intelligence Agencies), will confirm whether or not personal data is held. The department will inform the ICO either that (i) this information relates to the Security and Intelligence Agencies, or (ii) that the information does not relate to the Security and Intelligence Agencies, in which case it will explain in general terms why it is necessary to withhold the personal data requested in order to safeguard national security;
- (c) in cases where exemption in section 28 of the DPA is relied on to support a Neither Confirm Nor Deny response, will explain in general terms why it is necessary to neither confirm nor deny whether the requested information or personal data is held, in order to safeguard national security.

11. It is envisaged that in the vast majority of cases it will be possible to resolve the case by dialogue and correspondence between the Commissioner and the relevant Department(s). In other words, it is envisaged that a reasoned explanation, together with any relevant background information, normally by way of a letter from an appropriate person in the Department, will usually be sufficient to satisfy the Commissioner that the relevant exemptions have been properly relied on or that a Neither Confirm Nor Deny response has been properly given, without disclosing to the Commissioner the detailed content of the withheld information or personal data or, in a Neither Confirm Nor Deny case, without disclosing whether the information that has been requested is held and without recourse (on the Commissioner's part) to an Information Notice or (on the Department's part) to a Section 28 Certificate under the DPA.
12. In those exceptional cases where a reasoned explanation, together with any relevant background information, is (for whatever reason) not sufficient to satisfy the Commissioner, he will explain in writing why this is the case. It is recognised that it may be necessary for him to be granted confidential access to the withheld information or personal data or, in a Neither Confirm Nor Deny case, to be informed whether the requested information is held in order to satisfy himself that the relevant exemptions have been properly relied on or that a Neither Confirm Nor Deny response has been properly given. The process and requirements for Commissioner access to the information is set out in paragraphs 22-24.

## **Information Notices**

13. The Commissioner will generally only serve an Information Notice under section 43 of the DPA on any Department where:
  - (a) it has not been possible to resolve the case by agreement, and
  - (b) the Commissioner believes either:
    - (i) that relevant personal data is being withheld from him, for example, the personal data which is the subject of the complaint and which, in an exceptional case, he considers he needs to see in order to satisfy himself that the relevant exemptions have been properly relied on, or

- (ii) that there has been undue delay in providing such information or data to him.

14. Where the Information Commissioner intends to serve an Information Notice, wherever possible he will inform the Department and the Ministry of Justice in advance.

### **National Security Certificates**

15. Departments will seek a Ministerial Certificate under section 28 of the DPA only where:

- (a) the individual whose request for personal data has been refused, or an individual who is directly affected by the processing of their data by a Department, complains to the Commissioner, and
- (b) the Commissioner indicates that he requires a certificate and will issue an enforcement notice under section 40 of the DPA, or an information notice under section 43 of the DPA.

16. Generic or prospective certificates made under section 28 of the DPA exist in relation to personal data processed by the Security and Intelligence Agencies and may be used by other departments. The Security and Intelligence Agencies will similarly rely on such Certificates where:

- (a) the individual whose request for personal data has been refused complains directly to the Tribunal; or
- (b) the individual whose request for personal data has been refused complains to the Commissioner; and
- (c) the Commissioner indicates that he is minded to pursue the complaint and embark on the enforcement procedure under the DPA.

Where the relevant Security and Intelligence Agency proposes to rely on its Section 28 Certificate, then wherever possible it will inform the Commissioner in

advance.

## **The protection of information provided to the Commissioner in accordance with this MoU**

17. Where the Commissioner has received the withheld information or personal data in order to enable him to discharge his statutory obligations, such information or data will be held by him subject to the arrangements set out in paragraphs 18-24 of this MoU.
18. The Commissioner will not disclose to the Complainant or to any third party the reasoned explanation or any other information provided to him by a Government Department either under the terms of this MoU or as a result of serving a notice under section 40 or 43 of the DPA. In addition, except where expressly provided for under the DPA the Commissioner will not in any event disclose the withheld information or personal data covered by this MoU to the Complainant or any third party unless:
  - (a) the Department consents to the disclosure (after consultation), or
  - (b) all appeal proceedings have been exhausted.
19. Where release of such information seems to the Commissioner to be necessary under or in connection with any enactment, Community obligation, proceedings or otherwise, the Commissioner shall inform the Department and the Ministry of Justice as soon as possible.
20. Where the circumstances mentioned in paragraph 19 arise, the Commissioner acknowledges that he will resist release of the information, where in all the circumstances it is reasonable to do so, and by all reasonable means including the use of any appeals processes.
21. The Commissioner will ensure that any information that is protectively marked will be kept in accordance with the standards of security required by the Security Policy Framework (HMG's guidance on the protection of government assets, issued by the Cabinet Office) for as long as he retains the information

22. As described in paragraph 12, it is recognised that in exceptional circumstances it may be necessary for the Commissioner to seek and be granted access to the relevant information. In such cases, the Commissioner agrees to inspect at the premises of the relevant Department any papers which are particularly sensitive.
23. Where particular security or sensitivity considerations so demand, the Department may indicate that it would, in its view, be more appropriate for the Commissioner himself, or nominated members of the ICO staff (with the appropriate level of security clearance if necessary), to inspect the information. The Commissioner will take full account of such a view and will not refuse any such representations unless there are overriding reasons why adoption of such a procedure would significantly obstruct the discharge of his statutory functions.
24. The Commissioner will not hold information provided to him under this MoU for longer than is necessary for the discharge of his statutory functions. The Commissioner will, in consultation with the Department, arrange for the secure return or secure disposal of the information, in accordance with the Security Policy Framework.

#### **Processes on whether to issue an Enforcement Notice under the DPA**

25. The Commissioner will consider all information provided to him in reaching a decision whether to serve an Enforcement Notice under the DPA on the Department.
26. The Commissioner will contact both the Department and the Complainant, whenever appropriate, throughout his consideration of a complaint and, in any event, will normally provide progress reports every 28 days.
27. Wherever practicable in a national security case, the Commissioner will explore the scope for a settlement of the complaint, which would be acceptable to the Complainant and to the Department. Where such settlement can be achieved (by means, for example, of the provision by the relevant Department of an explanation in general terms of the sensitivity of the information requested), the Complainant will be invited to withdraw the complaint.

## **Draft Enforcement Notices under the DPA**

28. In view of the inherent sensitivity of national security cases, the Commissioner recognises the obligation on the ICO to avoid the disclosure of exempt information in Enforcement Notices. In cases where Departments raise specific concerns, the ICO will enter into appropriate consultation, including where necessary the provision by the ICO of the relevant extracts of draft text, in order to ensure that Enforcement Notices as published do not contain any information the disclosure of which would be likely to damage national security.

## **Enforcement Notices under the DPA**

29. If the Commissioner decides to issue an Enforcement Notice under section 40 of the DPA, he will serve the Notice on the Department and the Complainant simultaneously. He will give both the Department and the Complainant a reasonable period of time to digest the Enforcement Notice before making the Notice publicly available.

## **General**

30. Wherever possible and subject to the requirements to ensure the security of sensitive documents relating to national security or to personal data of a data subject, the Commissioner and Departments shall communicate by means of electronic communication.
31. This MoU will be kept under review and will be amended, as necessary, in the light of experience by agreement between the Participants.
32. The Ministry of Justice shall ensure that this MoU is widely disseminated within government and shall encourage compliance with it.

**Signed by:**

The Rt Hon Chris Grayling MP,  
Secretary of State for Justice  
on behalf of central Government  
Departments

CHRIS GRAYLING

---

Christopher Graham,  
Information Commissioner

CHRISTOPHER GRAHAM

---

**Dated:**

2 SEPTEMBER 2013

---

## **ANNEX: Definitions**

In this Memorandum of Understanding:

“The Participants” means the Secretary of State for Justice and the Commissioner.

“The MoJ” means the Ministry of Justice

“The Commissioner” means the Information Commissioner

“MoU” means Memorandum of Understanding

“Department” means a government department as defined in section 70(1) of the Data Protection Act 1998, the Security and Intelligence Agencies, the armed forces of the Crown, the Ministry of Defence Police and the Serious Organised Crime Agency. For the purposes of the operation of this MoU, the armed forces of the Crown and the Ministry of Defence Police are to be treated as part of the Ministry of Defence.

“The DPA” means the Data Protection Act 1998.

“The Tribunal” means the First-tier Tribunal (Information Rights).

“Complainant” means a person who has applied to the Commissioner for an assessment under section 42 of the DPA.

“Information Notice” and “Enforcement Notice” in relation to the DPA have the meanings assigned to them in the DPA.

“The Security and Intelligence Agencies” means the Security Service, the Secret Intelligence Service and the Government Communications Headquarters.